Department of Homeland Security Daily Open Source Infrastructure Report for 11 August 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

−− Only Two Days Left −− Please Help Improve the DHS Daily Infrastructure Report!!

We are striving to improve the DHS Daily Infrastructure Report for all of our readers. Please help us in this effort by filling out a short feedback form, which can be found by clicking on this link:

http://chrome.osis.gov/questionnaire

The form will only be available for *two more days*, so please fill it out at your earliest convenience. Your participation is important to us! Thank you.

Daily Highlights

- The Miami Herald reports that according to a recent study, about 20 percent of computer−related crime is generated by disgruntled company insiders against their unsuspecting bosses, resulting in the loss of hundreds of millions of dollars a year. (See item 7)
- The Associated Press reports President Bush has signed a highway bill authorizing $286.4 billion over six years for roads and bridges, rail and bus facilities, bike paths, and recreational trails. (See item 11)
- The Waterloo/Cedar Falls Courier reports the Department of Homeland Security and the nation's largest food bank network have signed an agreement to strengthen their coordination to prepare for and respond to natural or man−made disasters. (See item 25)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 10, Midwest ISO* — **Cooperation among electric grid operators helping to meet high demand for power.** Mid−way through a hot, humid summer, electric grid operators across much of the country have managed increased demand for power by coordinating their efforts to ensure reliability and maintain system performance. Grid operators responsible for managing the flow of wholesale power across the Eastern Interconnection −− an area that stretches from the Rockies to New England and from Arkansas to Manitoba −− have all reported record levels of electricity usage during this summer's extreme heat and high humidity. Thus far, their systems have met demand with few problems, although some organizations have asked consumers to conserve power during periods of peak usage. The grid managers credit coordinated efforts with their own members and with other independent system operators, or ISOs, for their continued ability to meet high demand and to maintain system performance and reliability. Numerous operating agreements between ISOs have improved coordination, particularly at seams along the borders of neighboring systems. Under the agreements, the ISOs share critical operating data relating to the management of reliability and relief of congestion within their respective systems.
Source: http://www.midwestmarket.org/publish/Document/2b8a32_103ef71 1180_−78ca0a48324a/2005−08−10%20prs%20rel%20−%20Joint%20heat %20wave%20release%20FINAL.pdf?action=download&_property=Atta chment

2. *August 10, The Janesville Gazette (WI)* — **Electricity use sets record, according to energy company.** Alliant Energy has reported a new record for electricity used in a day. The new peak demand for energy was set about 4 p.m. Tuesday, August 9, by Wisconsin Power & Light Co. (WP&L) customers. Alliant reported that customers used about 2,830 megawatts of electricity, nine above the previous record set last week. The power demands were met and did not interrupt anyone's service, according to an Alliant release. The Tuesday high in Janesville was 96 degrees. This was the hottest August 9 since 1949, when temperatures reached 100 degrees, according to Janesville Gazette weather records. WP&L is a subsidiary of Alliant.
Source: http://www.gazetteextra.com/alliant081005.asp

3. *August 10, RenewableEnergyAccess.com* — **World's largest solar project unveiled.** A partnership between Stirling Energy Systems (SES) and Southern California Edison (SCE) would see the construction of an expansive 4,500−acre solar generating station in Southern California. When completed, the proposed power station would be the world's largest solar facility, capable of producing more electricity than all other U.S. solar projects combined. The 20−year power purchase agreement signed today, which is subject to California Public Utilities Commission approval, calls for development of a 500 MW solar project 70 miles northeast of Los Angeles using innovative Stirling dish technology. The agreement includes an option to expand the project to 850 MW. "At a time of rising fossil−fuel costs and increased concern about greenhouse−gas emissions, the Stirling project would provide enough clean power to

serve 278,000 homes for an entire year," said SCE Chairman John Bryson. Although Stirling dish technology has been successfully tested for 20 years, the SCE−Stirling project represents its first major application in the commercial electricity generation field.
Source: http://www.renewableenergyaccess.com/rea/news/story;jsessionid=a5x_Y−baZwO9?id=35263

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *August 10, The Des Moines Register (IA)* — **Chemical blast at plant burns two.** Investigators said Tuesday, August 9, that an explosion at a Story City, IA, packaging plant was sparked in a room where an employee was washing unidentified chemicals from a pail. Two employees suffered burns on Monday, August 8, at a blast at American Packaging Corp. One person suffered broken legs from a door that was blown open, said Dennis Appelhons, an environmental specialist for the Iowa Department of Natural Resources. Police and fire officials said they did not know the names of those injured at the plant, which makes food packaging. Company officials refused to provide details of what happened. Appelhons said employees at the plant routinely wash five−gallon pails, but "the curious part is finding out what actually sparked this flash explosion." The impact of the blast collapsed the floor and caused a steam tank to fall through, he said.
Source: http://www.dmregister.com/apps/pbcs.dll/article?AID=/20050810/NEWS04/508100376/1001

5. *August 10, Local 2 (TX)* — **Second leak in two weeks results in order for residents to stay indoors.** Officials with the BP refinery in Texas City, TX, said Wednesday, August 10, the second leak in as many weeks is not connected to two explosions that have occurred there this year The gas company said they still don't know what caused the leak, which sent a cloud of smoke over the area at 1 a.m. Bruce Clawson, the city's emergency management coordinator, said the heavy oil and gas leak occurred just after 1 a.m. in the Cat Feed Hydro Unit. Residents near the refinery were asked to shelter−in−place because of the leak after Texas City firefighters and emergency management coordinators issued a Level 3 alert. "Level 3 means it has impacted the community to some degree −− in this case, the mixture was going across parts of the city. We sounded the siren system to advise people to shelter−in−place," Clawson said. The Level 3 order to stay indoors was lifted about 2:30 a.m. after officials said the leak was contained. The Texas City Fire Department monitored the air and found no indication of toxic or harmful materials, Clawson said.
Source: http://www.click2houston.com/news/4831926/detail.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *August 10, Associated Press* — **London financial area may be terror target.** The police chief for London's financial district warned Wednesday, August 10, that terrorists will likely strike the British capital's biggest business hub, where they have already surveyed targets in the area. Nearly five weeks after four suicide bombers attacked London, killing themselves and 52 other people, James Hart said there was no specific intelligence about a forthcoming attack but insisted the district was at risk. "We are vulnerable, there are people out there who wish us harm and we should be aware of that," the police chief said. "If you hit the financial center of the United Kingdom, it's a high−profile thing to do," said Hart. Known as the City, London's business quarter houses hundreds of banks, insurance companies, law firms and other institutions, including the London Stock Exchange and the Bank of England. It is a leading international center for trading in metals, oil and other commodities.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/08/10/AR2005081000369.html

7. *August 10, Miami Herald* — **Secret Service targets sabotage.** About 20 percent of computer−related crime is generated by disgruntled company insiders against their unsuspecting bosses, resulting in the loss of hundreds of millions of dollars a year, according to a study presented on Tuesday, August 9, during a training session for the U.S. Secret Service's Miami−based Electronic Crimes Task Force. "This is something that's been overlooked for quite a while," said William Sims, special agent in charge of the Miami field office. It used to be attacks from the outside for financial gain. These are attacks from the inside," said Sims. Dawn Cappelli of Carnegie Mellon University's Software Engineering Institute and her colleagues found that saboteurs fit no definitive psychographic profile other than being poor performers in some way at work and technically savvy. Employees to especially watch out for are high−level information technology specialists who have wide−ranging access to the company's systems, she said. The seminar marked the rollout of the Secret Service's insider threat training program, which is planned to be offered to other e−crime task forces across the country. The sessions are based on a recently−completed study by the Secret Service's National Threat Assessment Center and software experts from Carnegie Mellon University.
   Insider Threat Study: http://www.secretservice.gov/ntac_its.shtml
   Electronic Crimes Task Force: http://www.ectaskforce.org/index.htm
   Source: http://www.philly.com/mld/miamiherald/news/breaking_news/12343050.htm?source=rss&channel=miamiherald_breaking_news

[Return to top]

Transportation and Border Security Sector

8. *August 10, USA TODAY* — **Independence Air may be near Chapter 11 filing.** Fourteen months after launching, discount carrier Independence Air warned Tuesday, August 9, it's preparing for a possible Chapter 11 bankruptcy filing. In a securities filing, the Washington, DC−based carrier didn't rule out the possibility it might liquidate. Battered by fare wars and record high fuel prices, Independence Air also reported a $98 million loss for the second quarter, more than triple its $27 million loss a year ago. Its cash balance plummeted 61% in the

first half of this year to a dangerously slim $65 million. Company officials said the carrier hopes to borrow cash, but they weren't optimistic. Independence Air is the latest U.S. airline to warn it might face a bankruptcy filing this fall, but its warning is the most dire. Although Delta and Northwest also have warned of possible filings, neither faces the prospect of liquidation. Source: http://www.usatoday.com/travel/news/2005−08−09−indy−air−usat_x.htm

9. *August 10, TheBostonChannel (MA)* — **Logan officials unveil plan for safer runways.** New signs and closer supervision of planes as they taxi along the runways at Boston's Logan International Airport are among the safety precautions being taken following a series of incidents on Logan's intersecting runways. So far this year, Logan has seen 12 so−called "incursions," in which planes have been cleared for takeoff only to find another aircraft blocking the runway. Only one of those was considered serious −− an incident involving two passenger jets that narrowly avoided a high−speed collision. Still, the most recent incursion earlier this week prompted officials from the Federal Aviation Administration and the Massachusetts Port Authority (Massport), which manages Logan, to unveil a new runway safety plan on Wednesday, August 10. The safeguards include new signs that will better indicate where planes should stop. Also, a Massport official will escort all planes being moved around the airport. The chief pilots from several airlines will meet next week to discuss the new procedures. Experts say Logan has a higher−than−average number of incursions in part because of its cramped layout. The nation's 17th busiest airport is located on a mostly man−made peninsula jutting into Boston Harbor, with five runways, all of them intersecting.
Source: http://www.thebostonchannel.com/news/4834427/detail.html

10. *August 10, Local 6 News (FL)* — **Package from 'bin Laden' on Orlando bus investigated.** Bomb experts were called to a Lynx public bus in Orlando, FL, Wednesday, August 10, after a suspicious package addressed from Osama bin Laden was discovered by a rider, according to police. The bus usually travels around downtown Orlando. When the driver saw that Osama bin Laden was written on the package, he called 911, Local 6 News reported. Firefighters and police aggressively moved into the area and checked the package. Several streets in the downtown area were closed. The package was packed with flyers but police did not say what the flyers said. Orlando fire officials said they have had several incidents like this where suspicious packages have been left in places with the intention of causing alarm, Local 6 News reported. "Because of handwriting on the packages and other details, they believe the same person is responsible," Local 6 News reporter Louis Bolden said.
Source: http://www.local6.com/news/4833261/detail.html

11. *August 10, Associated Press* — **Bush signs huge highway bill.** President Bush on Wednesday, August 10, signed a bill authorizing $286.4 billion over six years for roads and bridges, rail and bus facilities, bike paths, and recreational trails, saying the projects from coast to coast would spur the economy and save lives. Lawmakers backing the bill say money for infrastructure is well spent, especially considering that traffic congestion costs American drivers 3.6 billion hours of delay and 5.7 billion gallons of wasted fuel every year. Substandard road conditions and roadside hazards are a factor in nearly one−third of the 42,000 traffic fatalities a year, officials say. "This bill upgrades our transportation infrastructure and it'll help save lives," Bush said. The president touted a provision that gives states incentives to increase seat belt usage and create vehicle stability standards by 2009 to prevent rollovers. And he noted that with this bill, the federal government is not raising gas taxes to pay for road projects as some have advocated.

Source: http://www.cnn.com/2005/POLITICS/08/10/bush.highwaybill.ap/

12. *August 07, New York Times* — **High−tech efforts to track border crossings.** Hoping to block the entry of criminals and terrorists into the United States and to improve the enforcement of immigration laws, government officials have in the past several years created enormous new repositories of digitally recorded biometric data that can be used to identify more than 45 million foreigners. Although the immigration control and antiterrorism campaign effort has fallen short of its goals, in the past year, thanks to a new system that allows Border Patrol agents to check quickly and comprehensively the fingerprints of every illegal immigrant detained near the border, officers have identified 437 people wanted, previously charged or convicted of homicide; 579 who had sexual assault records and more than 18,000 others with records involving robberies, drugs, kidnappings or assaults. The science of biometrics relies on unique human characteristics −− including fingerprints, facial dimensions or the rings and furrows in the colored tissue of the eye −− that can verify a person's identity. The high cost comes from the extensive computer networks that must be built to tie together the data and make it accessible to United States officials around the world.
Source: http://www.nytimes.com/2005/08/10/politics/10biometrics.html ?hp&ex=1123732800&en=09705d9255cb76e8&ei=5094&partner=homepa ge

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *August 10, Illinois Ag Connection* — **New state law to protect Illinois' agriculture assets.** Governor Rod Blagojevich Tuesday, August 9, signed into law new penalties to deter the vandalism of farmland and farm equipment and to protect the state's important agricultural production. House Bill 120 was introduced after vehicles on three farms in Macon County and one farm in McLean were deliberately set on fire in the fall of 2003, collectively causing about $400,000 damage and hampering farmers' ability to harvest their crops. The law makes criminal damage to such equipment and "immovable items of agricultural production" like barns and grain bins a felony offense. It also stiffens the penalty for trespassing on farms from a Class B to a Class A misdemeanor, effectively doubling the potential jail time for the crime from six months to one year and increasing the maximum fine from $1,500 to $2,500. Also under HB 120, penalties for vandalizing farm equipment escalate according to the dollar value of the damage. If the damage totals $300 or less, the crime is a Class 4 felony punishable by one to three years in prison. However, damage exceeding $100,000 is a Class 1 felony, which carries a possible prison term of four to 15 years.
Source: http://www.illinoisagconnection.com/story−state.cfm?Id=626&y r=2005

14. *August 09, Stop Soybean Rust News* — **Rust found in Escambia sentinel plot.** Alabama officials report that soybean rust was found Monday, August 8, in a soybean sentinel plot in

Escambia County. There are now four counties in the state with rust, Escambia in the southwest and the adjacent county Baldwin, and Elmore and Lee in the east−central region. As a point of information, Escambia County in Florida also has rust this year. It borders its namesake county in Alabama to the north, and Baldwin County, Alabama to the west −− making a cluster of three contiguous large counties with rust in that area.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=498

15. *August 09, Animal and Plant Health Inspection Service* — **Final recommendations on safeguarding plant resources adopted.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service, plant protection and quarantine (PPQ) program, Tuesday, August 9, released its fourth and final report, Safeguarding Implementation −− A Time for Celebration and Reflection, announcing its implementation of more than 300 recommendations for bolstering protection of U.S. agriculture and plant resources from destructive, nonnative plant pests. The recommendations were the result of an 11−month study conducted in 1999 by the National Plant Board, a consortium of state regulatory agencies. Developed by a 43−member review group comprised of representatives of state government, industry, academia, and advocacy groups, the recommendations addressed four primary components of PPQ's safeguarding system −− the collection and use of international pest information; the use of permits to manage risk; the exclusion of pests; and the detection of and response to pests that enter the U.S. Over the past five years, PPQ has worked diligently and systematically toward achieving the safeguarding review's recommendations. To date, every recommendation in the safeguarding review has been fully evaluated. Most recommendations are either implemented or in the process of being implemented. A small number of recommendations were referred to the Department of Homeland Security's Customs and Border Protection after the 2003 transfer of the agricultural inspection mission to the agency.
Source: http://www.aphis.usda.gov/lpa/news/2005/08/safeguar_ppq.html

[Return to top]

Food Sector

16. *August 10, USAgNet* — **Food and Drug Administration considering more feed protection regulations.** The U.S. Food and Drug Administration (FDA) will propose new regulations designed to provide additional protection in the U.S. livestock feed supply against bovine spongiform encephalopathy (BSE). FDA is focusing on eliminating specified risk materials from all animal feed to remove the risk that brain and spinal cord tissue from cattle 30 months old or older would be in the feed. Research has shown that older cattle are the most at risk for developing BSE. The proposed new rules will address lingering questions about feed compliance, the recently named administrator of FDA, Lester Crawford, told a gathering of meat scientists in Baltimore, MD.
Source: http://www.usagnet.com/story−national.cfm?Id=800&yr=2005

17. *August 04, Fort Morgan Times (CO)* — **Officials institute new policy for Colorado's feeder cattle.** Officials at the Colorado Department of Agriculture have instituted a new policy for feeder cattle. On July 15, the U.S. Department of Agriculture reopened the U.S. border to Canadian cattle and other ruminants under 30 months of age when they arrive at market. Within the Colorado Canadian Feeder Cattle Import Policy, the feeder cattle and the feedlots receiving

the cattle have to meet specific requirements. Cattle must be 30 months of age or younger at the time they go to market. Cattle must have Canadian radio frequency identification (RFID) or barcode ear tags. All feeder cattle must be properly hot branded on the right hip with the Canadian brand. Feedlots receiving the cattle must have an official premises identification number prior to receiving cattle. Animals' IDs must be recorded with the premises in the state database. Trucks transporting cattle must arrive sealed. Upon arrival at the feedlot, state officials will read the IDs that include bar codes, RFID and visual tags. Cattle without an RFID tag will have one applied. Cattle going to a meat processing facility will be transported in a sealed truck from the feedlot. These animals cannot be older than 30 months of age, and the animal ID will be recorded and retired at slaughter.
Source: http://www.fortmorgantimes.com/Stories/0,1413,164~8305~29962 06,00.html

[Return to top]

Water Sector

18. *August 10, Casper Star−Tribune (WY)* — **Wyoming plans cloud seeding.** Despite skeptics within the scientific community and a well−publicized history of failure during the 1970s, Wyoming is ready to go ahead with a new five−year, $8.9 million cloud−seeding project, state officials told the Platte River Basin Advisory Group Tuesday, August 9. The project is to be one of the best funded and best researched cloud−seeding attempts in the U.S., officials from the Wyoming Water Development Commission said, and parts of Wyoming should see a direct increase in snowpack of at least 10 percent due to the program. It could begin as soon as this winter. The Sierra Madre, Medicine Bow and Wind River mountain ranges are the targets for the state−funded "weather modification" project. It aims to increase snowfall by releasing a silver iodide compound into the clouds around the ranges using fixed platforms and special aircraft. According to the commission, which oversees the project, while the cloud seeding would only occur during winter, the increased snowpack in the mountains should yield at least 130,000 to 260,000 acre feet of additional runoff per season.
Source: http://www.casperstartribune.net/articles/2005/08/10/news/wyoming/88a1439bdb1f95b3872570580081e554.txt

19. *August 09, Associated Press* — **Kansas starts pilot program on water banking.** David Pope, chief engineer for the Kansas Division of Water Resources, announced Tuesday, August 9, he signed the paperwork creating the state's first water bank charter for groundwater users in south−central Kansas. In Kansas, water use other than for household consumption requires a water right permit, setting out how much water can be used each year at a specific location and its intended use. It can only be used for such things as irrigation, watering crops and livestock, or providing water to residents or industries. Through the bank charter, water rights holder can "deposit" water they won't be using in coming years in exchange for payment or other compensation from the person wanting it. Those making the "deposit" continue to hold the water rights, which often remain in families for generations. Allowing others to use the water will require a minimum of 10 percent of the water to be conserved. That means for 100 acre feet of water on deposit, 90 acre feet will be available. The "deposit" can range from one year to five years and after that, the annual amount of water again is available to the water right holder.
Source: http://www.kansas.com/mld/kansas/news/state/12342297.htm

[Return to top]

Public Health Sector

20. *August 10, Agence France Presse* — **World Health Organization (WHO) close to setting up global stockpile of anti−flu drugs.** The World Health Organization (WHO) efforts to build up a global stockpile of at least one million doses of an anti−flu drug to tackle a threatened pandemic could bear fruit soon, the Swiss pharmaceutical firm Roche said. Roche and the WHO have been holding talks on additional stockpiles of the drug oseltamivir −− sold under the brand name Tamiflu. National reserves are being built up by at least 25 countries on three continents. The WHO is unusually also aiming to set up an emergency stock in order to react swiftly to a new pandemic strain of influenza when it appears, especially in poorer countries that are ill−prepared. Concern about the imminent appearance of a deadlier and far more infectious type of flu in humans has grown with the spread of the H5N1 strain of bird flu in poultry or wildfowl in Asia and parts of the ex−Soviet Union. While research into a vaccine is ongoing, anti−viral drugs are thought to be an effective way of smothering a pandemic strain when it appears, provided the intervention is swift. Currently, the WHO only has a small reserve of a few doses to protect staff who intervene in emergencies and has urged countries to bolster their own preparations. Roche has quadrupled production capacity for the antiviral capsules in the past two years.
Source: http://news.yahoo.com/s/afp/20050810/hl_afp/healthfluwhopharmacompanyrochedrugs_050810115310

21. *August 10, Xinhua (China)* — **Pigs vaccinated against epidemic in Sichuan.** China began to inoculate pigs Wednesday, August 10, with newly−developed vaccines in south China's Sichuan Province in an effort to prevent the spread of streptococcus suis, according to the provincial animal husbandry bureau. The streptococcus swine type II, produced by a company in the southern province of Guangdong and another Sichuan−based firm, will be injected in pigs in accordance to fixed schedule. With the approval of the Ministry of Agriculture, the compulsory vaccination will start from areas without pig−borne disease cases and gradually lead to regions afflicted by the bacteria, which has infected humans in many villages and towns.
Source: http://news.xinhuanet.com/english/2005−08/10/content_3336173 .htm

22. *August 10, Greeley Tribune (CO)* — **Six cases of Q fever reported in Colorado.** Six Q fever infections in Weld, CO, more than any other county in the state, at first seemed like a big deal, since in rare cases, the disease can be fatal, and there were a mere three cases in Colorado last year. With six reports in Weld this season, the Weld and state health departments, along with the department of agriculture went into its bioterrorism mode in case the sudden hike in infections was terrorist−related. After a swift investigation, they discovered it wasn't, but it was good practice, said Jill Burch of the Weld County Department of Public Health and Environment. Q fever is on the list of possible bioterrorism agents. It is an animal−borne disease spread by direct contact with infected animals' milk, urine, feces, and birthing fluids. The disease causes high fever, severe headaches, and diarrhea. Only in rare cases will a person develop a chronic condition that can lead to heart conditions. A cluster of six infections was alarming enough to investigate the source, Burch said. But they never considered it would be a bioterrorism−related. Several of the infections were within one family.

Q fever information: http://www.cdc.gov/ncidod/diseases/submenus/sub_q_fever.htm
Source: http://www.greeleytrib.com/article/20050810/NEWS/108100060

23. *August 10, Interfax (Russia)* — **Forty−nine hospitalized with unknown infection in Udmurtia.** Forty−nine people in the village of Sharkan in the Russian internal republic of Udmurtia have contracted an unknown infectious disease, the regional civil defense and emergency situations center reported on Wednesday, August 10. According to the report, 41 people were hospitalized in Sharkan and eight in the republic's central clinical hospital in Izhevsk.
Source: http://www.interfax.ru/e/B/politics/28.html?id_issue=1136139 5

24. *August 09, Weschester.com (NY)* — **Computerized surveillance system tracks disease.** It may not seem too likely, but what if a number of people in Westchester, NY, began experiencing similar symptoms but all reported to different clinics and hospitals? How long would it take for someone to put two and two together and realize there's a pattern of illness. Probably not too long, given a computerized early warning surveillance system developed by the Westchester County Departments of Information Technology (DoIT) and Health. The Community Health Electronic Surveillance System, or CHESS, was initiated by the county as part of an overall push to use technology to make residents safer. While there have fortunately been no large−scale public health emergencies, CHESS has identified the beginnings of flu season the past two winters, searched for Severe Acute Respiratory Syndrome patients, looked for food illnesses during the 2004 blackout, and caught the "Clinton effect" −– a spike in the number of patients reporting to emergency rooms with chest pain following revelation of the former president's heart problems. Following two years of effort and coordination with medical facilities, all the hospitals in Westchester with emergency departments and selected outpatient clinics are now participating in the program. CHESS gets numbers from hospitals on a daily basis and statistically analyzes any unusual levels or patterns of disease.
Source: http://westchester.com/Westchester_News/Westchester_Health_News/Computerized_Surveillance_System_Tracks_Disease_20050809 5528.html

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

25. *August 10, Waterloo/Cedar Falls Courier (IA)* — **Food banks link up with Department of Homeland Security.** The Department of Homeland Security and the nation's largest food bank network, with a branch in Waterloo, IA, signed an agreement Tuesday, August 9, to strengthen their coordination to prepare for and respond to natural or man−made disasters. Leaders of America's Second Harvest and the Federal Emergency Management Agency (FEMA), which is part of the homeland security agency, finalized a proposal two years in the making, essentially allowing the U.S. government to use the resources of local food banks for disasters from floods

to terrorist attacks. The two organizations also will create plans to coordinate community involvement for emergencies. "Each piece of the disaster−assistance pie is equally important and is equally depended upon by the American people," said FEMA head Michael Brown. The agreement, signed at FEMA headquarters, is effective immediately.
Source: http://www.wcfcourier.com/articles/2005/08/10/news/politics/e7470d1181d1f28386257059004befd2.txt

[Return to top]

Information Technology and Telecommunications Sector

26. *August 09, FrSIRT* — **Gravity Board X SQL injection and file inclusion vulnerabilities.** Two vulnerabilities have been identified in Gravity Board X, which could be exploited by attackers to include arbitrary files and/or conduct SQL injection and cross site scripting attacks. The first issue is due to an input validation error in the "deletethread.php" script when processing a specially crafted "board_id" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. The second vulnerability is due to an input validation error in the "index.php" script that does not properly filter a specially crafted "email" variable, which may be exploited by remote users to conduct SQL injection attacks. The third flaw is due to an input validation error in the "editcss.php" script when processing a specially crafted "csscontent" variable, which could be exploited by attackers to execute arbitrary PHP commands. Gravity Board X version 1.1 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/1349

27. *August 09, Security Focus* — **AOL client software local privilege escalation vulnerability.** AOL client software is susceptible to a local privilege escalation vulnerability. This issue is due to a failure of the software to properly secure its installation path against local modifications. This issue allows local users to replace the affected binary with an executable of their choice, allowing them to execute arbitrary code with SYSTEM privileges. This facilitates the complete compromise of the local computer. AOL version 9.0 Security Edition is reported susceptible to this vulnerability; other versions may also be affected. Security Focus is not currently aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/14530/discuss

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports Microsoft has released security updates for Windows and Internet Explorer. To obtain the updates, visit the Microsoft Update web site. US−CERT also recommends enabling Automatic

Updates. Microsoft Security Bulletins for August, 2005 address vulnerabilities in Windows and Internet Explorer. These vulnerabilities may allow an attacker to take control of your computer or cause it to crash. For more technical information, see US−CERT Technical Cyber Security Alert TA05−221A. US−CERT also reports a remotely exploitable vulnerability in AWStats this was posted on Full Disclosure today at URL: http://seclists.org/lists/fulldisclosure/2005/Aug/0237.html US−CERT has seen past unauthorized access compromises due to AWStats compromises please make sure that your respective agencies / webmasters are notified. Additionally, if your site does not require/use AWStats please remove this tool. AWStats is a free tool that generates web, streaming, ftp or mail server statistics graphically. The vendor was originally made aware of this on May 12, 2005; a CVE has been assigned: CAN−2005−1527, and the vulnerability was fixed in release 6.4.

Current Port Attacks

Top 10 Target Ports	1026 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 6346 (gnutella−svc), 139 (netbios−ssn), 135 (epmap), 53 (domain), 1434 (ms−sql−m), 4672 (eMule), 32772 (sometimes−rpc7) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

28. *August 10, Wall Street Journal* — **Shopping for security at nation's malls.** The recent suicide bombings in London's mass−transit system have heightened fears in counterterrorist circles of similar attacks in America. Federal officials stress that there is no specific information that suicide bombers are poised to strike in the U.S. After the first London attacks on July 7, the Department of Homeland Security (DHS) raised the terror alert threat level for mass transit. On July 18, DHS sent federal agencies and state officials a collection of Central Intelligence Agency threat assessments listing malls, banks, prominent companies, and tall buildings as being soft targets most at risk of being bombed. The possibility of suicide attacks against the nation's 1,200 enclosed shopping centers, bustling icons of U.S. wealth and consumerism, is still only a grim theory. But the mere idea has transformed the way private security companies train their guards and go about their business. When the Department of Homeland Security sent out teams of threat−assessment experts −− many of them former Navy SEALs −− to the nation's malls in 2003, their recommendations seemed so extreme that industry officials balked. Among the recommendations for malls around the country were limiting the number of entrances, placing metal detectors at each door and screening shoppers for weapons.
Source: http://www.courant.com/business/hc−mallsecurity.artaug10,0,3012674.story?&track=rss

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.